(19)日本国特許庁（ＪＰ）　(12) **公表特許公報（Ａ）**　(11)特許出願公表番号

特表平11－500241

(43)公表日　平成11年(1999)１月６日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６５０	Ｇ０９Ｃ　1/00	６５０Ｚ
			６５０Ｂ

審査請求　有　　予備審査請求　有　（全 34 頁）

(21)出願番号　特願平9－518885
(86)(22)出願日　平成８年(1996)10月31日
(85)翻訳文提出日　平成10年(1998)５月18日
(86)国際出願番号　ＰＣＴ／ＵＳ９６／１７４４９
(87)国際公開番号　ＷＯ９７／１８６５２
(87)国際公開日　平成９年(1997)５月22日
(31)優先権主張番号　０８／５５９，２１３
(32)優先日　1995年11月16日
(33)優先権主張国　米国（ＵＳ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＣＡ，ＪＰ

(71)出願人　ベル　コミュニケーションズ　リサーチ，インコーポレイテッド
アメリカ合衆国　07960　ニュージャージー州　モーリスタウン　サウス　ストリート　445
(72)発明者　アイエロ，ウイリアム，エイ．
アメリカ合衆国　07940　ニュージャージー州　マディソン　メイプル　アヴェニュ　54
(72)発明者　ヴェンカテサン，ラマラスナン
アメリカ合衆国　07960　ニュージャージー州　モーリスタウン　コンクリン　アヴェニュ　9
(74)代理人　弁理士　谷　義一　（外３名）

(54)【発明の名称】　ハッシュ関数および疑似ランダム関数の安全性を高める効率的な暗号ハッシュ関数および方法

(57)【要約】
暗号ハッシュ関数回路（３００）はテーブル（３０１，３０２，…，３０３）を有しており、テーブル（３０１，３０２，…，３０３）への入力パス（３１１，３１２，…，３１３）上の入力$c_i(j)$を有し、出力パス（３２１，３２２，…，３２３）上への出力を作成して、排他的論理和ゲート（３３１）へ印加する。排他的論理和ゲートの出力は、パス（３５１）上のk_jである。キーＫは８個のk_jの連結である。

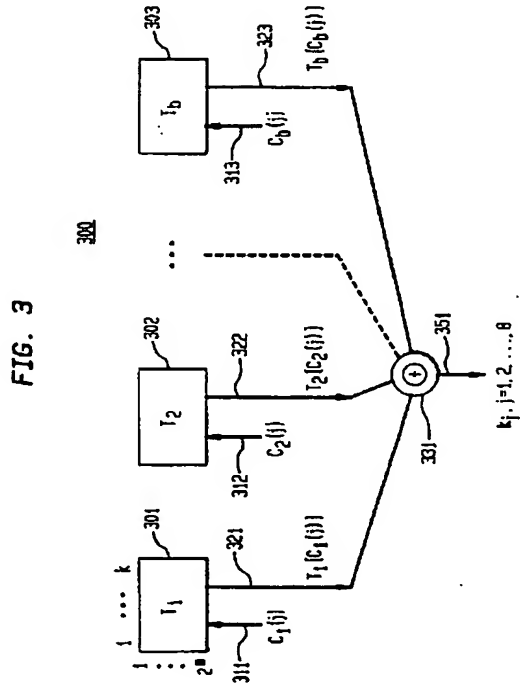

FIG. 3